Magistrate Judge Theiler

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA, Plaintiff, v. VOLODYMYR KVASHUK, Defendant.	NO. MJ19-321 MEMORANDUM IN SUPPORT OF MOTION FOR DETENTION

The United States of America, by and through Brian T. Moran, United States Attorney for the Western District of Washington, and Michael Dion, Assistant United States Attorney, files this memorandum in support of its motion to detain Defendant Volodymyr Kvashuk.

I. SUMMARY

Volodymyr Kvashuk, a former Microsoft employee, is charged with embezzling $10 million from the company. Kvashuk is a serious flight risk. He is a Ukrainian citizen and does not have permanent status in the United States. The Ukraine does not allow extradition of its citizens – indeed, the Ukrainian constitution specifically forbids it. Kvashuk, who faces a long prison sentence in this case, has great incentive to return to his home country – where his family lives, where he has spent most of his life, and where

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

he would be beyond the reach of U.S. law enforcement.

Furthermore, Kvashuk may well have the means to flee. His total profit from the fraud is unknown, but could be as high as $10 million. Law enforcement has only identified about $2.8 million. Kvashuk is a sophisticated user of cryptocurrency who has taken steps to conceal the money trail from his crime. He could have millions hidden somewhere. Indeed, agents found a note in his house outlining his plans to spend $10 million, as well as evidence of accounts and bitcoin wallets that may hold additional proceeds.

II. FACTS

A. Kvashuk's Background and Immigration Status

Kvashuk is a twenty-five year old Ukrainian software engineer. He was born in Rivne, where his father still lives and teaches at the National University of Ostroh Academy. Kvashuk earned a Bachelor's and Master's degrees in Economics and Cybernetics from that University in 2015.

Kvashuk arrived in the United States on a temporary B-2 visa in April 2015. Since his arrival, he has worked at several tech companies in various roles related to software engineering. He began work for Microsoft Corporation ("Microsoft") through a vendor from August 2016 to October 2017. Microsoft hired him as an employee in December 2017. In June 2018, the company uncovered the fraud and fired Kvashuk.

Kvashuk has overstayed his visa. He told Pretrial Services that he is applying for asylum.

B. Kvashuk's $10 Million Embezzlement Scheme

As explained below, Kvashuk used his position as a member of the Microsoft team that tested the company's online store to steal $10 million from the company.[1]

[1] Additional details are in the Complaint of Special Agent Michael Spiess.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Background of the testing program

Microsoft offers products and services to the public via its online store. To order from the store, a customer must create an account and link the account to (1) an email address, and (2) a credit card or other payment instrument.

The testing program was designed to simulate the experience of a customer trying to order products or services from the Microsoft online store. Testers would set up a test store account, which would be linked to a test email account and a fake credit card. The group that ran the testing, the Universal Store Team or "UST" team, would "whitelist" the test account, meaning that the account would bypass the company's normal security protections and data retention protocols.

Kvashuk's scheme exploited a vulnerability in the testing program. The program was set up to ensure that no physical goods would be delivered when orders were placed by test accounts, but there was no safeguard to prevent the delivery of digital currency ("currency stored value" or CSV), such as digital gift cards. A tester could use a test account to order CSV, and would get a code that could be redeemed and used to buy products or services from the MS store.

Kvashuk discovered this flaw and launched his scheme. At first, Kvashuk used his own test account to steal relatively small amounts of CSV. Eventually, Kvashuk expanded his scheme, and used accounts belonging to other testers to steal $10 million in CSV.

Kvashuk's Early Thefts Using His Own Test Account

The test account that MS set up for Kvashuk was called the "vokvas" test account. Kvashuk used the vokvas account to steal about $12,000 during the early phase of his scheme, from April to October of 2017. Although Kvashuk used his own test account to purchase the CSV, he generally used store accounts that were not in his name to redeem the CSV and make purchases from the Microsoft store. In one case, for example, Kvashuk appears to have used CSV to purchase products under the alias "Grigor Shikor."

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Microsoft investigators interviewed Kvashuk in May of 2018. Kvashuk admitted to using his test account to purchase CSV, and also admitted to using that CSV to purchase (or attempt to purchase) some products. Kvashuk claimed that he was not given clear instructions about what he could and could not purchase with his test account, and said that that he thought it was permissible to take CSV because it is not "real money."

Expansion of the Scheme Via Other Testers' Accounts

When Kvashuk first joined the testing team, he was working for a Microsoft contractor. His contracting job ended on October 1, 2017. Microsoft hired him as a direct employee (again on the testing team) on December 1, 2017.

Shortly before he joined Microsoft as a direct employee, Kvashuk ramped up the scale of the fraud and took new steps to hide his identity.

Starting on November 26, 2017, Kvashuk stopped using his own test account to purchase CSV, and began using accounts belonging to other testers. He continued using other testers' accounts until March 23, 2018, and stole about $10 million during that time.

Kvashuk knew that, although he was using other testers' accounts, his IP address might lead investigators to him. His internet search history shows that Kvashuk researched ways to anonymize himself online. Kvashuk used IP proxy services that concealed his true IP address when logging into the other testers' accounts. Records show that Kvashuk used these same proxy services to log into his personal email account and his Coinbase cryptocurrency account.

Unexplained Wealth

At least some of the stolen CSV was resold on overseas reseller websites to third parties. Investigators have not yet been able to get records from these sites. However, CSV sold on these reseller sites was traced back to CSV stolen from Microsoft. Records of Kvashuk's Internet search history show that – only days before Kvashuk began buying CSV in other testers' names – Kvashuk was researching how to sell CSV online.

During the period of the fraud, Kvashuk gradually transferred about $2.8 million

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

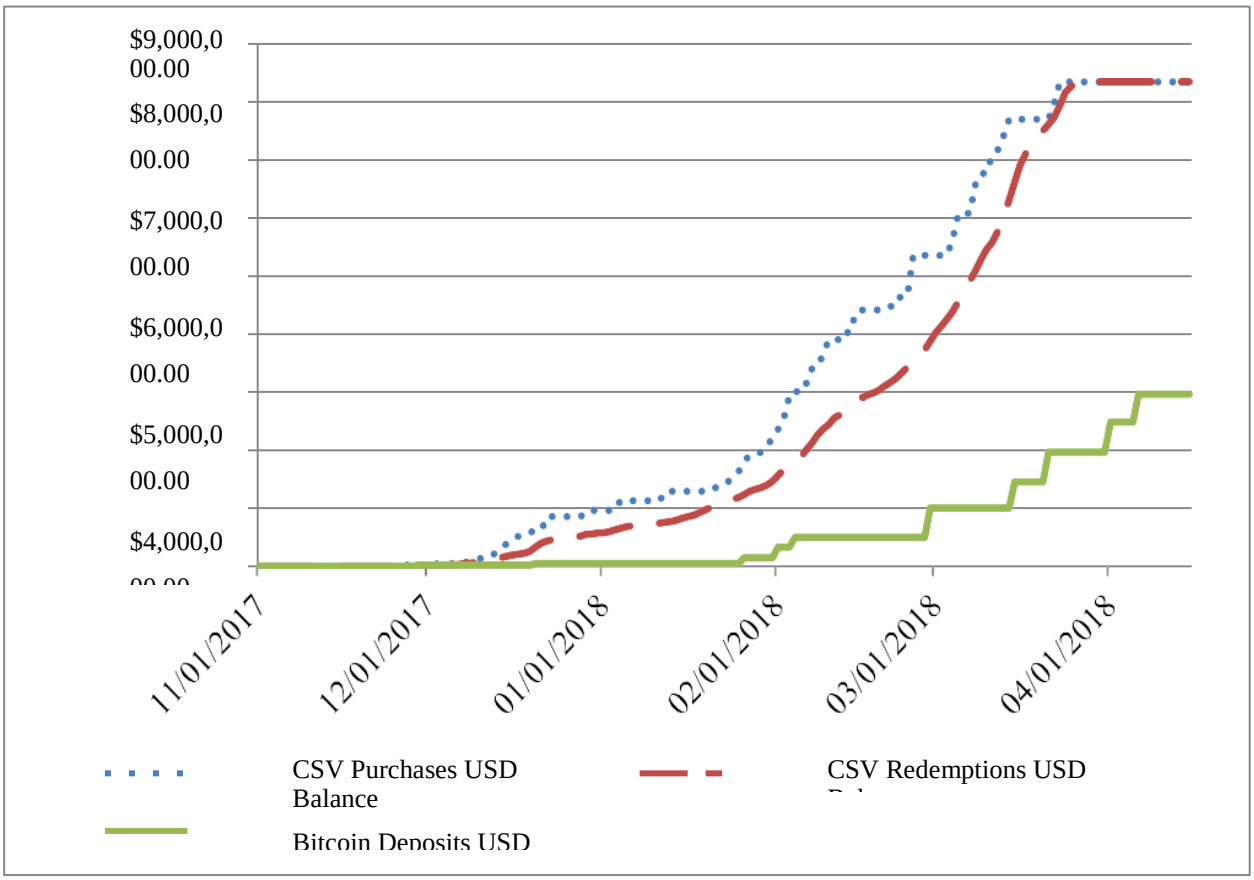
in cryptocurrency from his Coinbase bitcoin account to his bank and investment accounts. There are no records showing where the $2.8 million in bitcoin came from before it reached the Coinbase account, because Kvashuk used a "chipmixing" service that concealed the source of the bitcoin.

Kvashuk – who earned $116,000 a year at Microsoft – used this money to buy a $160,000 Tesla and a $1.6 million house in Renton. Kvashuk paid cash for the car and the house, with no financing.

As the chart below shows, Kvashuk's transfers from the Coinbase account to his bank and investment accounts correlate with the timing of the theft of CSV, and the timing of the redemption of the stolen CSV. As more CSV was stolen and redeemed, more money flowed into Kvashuk's accounts. The cash deposits in Kvashuk's accounts are a percentage of the total value of the stolen CSV, which could be explained by

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

fluctuations in bitcoin value, or by sale of the CSV at a discount.



Kvashuk did not report the $2.8 million on his tax returns. Records show that he told a tax preparer that the money was a gift from his father – a Ukrainian civil servant who earns about $1,000 a month.

7/16/19 Search and Arrest

Kvashuk was arrested at his house on July 16, 2019. He made no statements. Agents are continuing to review devices and other evidence. Agents found handwritten notes suggesting that Kvashuk has previously-unknown bank accounts, and one or more previously unknown bitcoin wallets. Nobody knows what is in those accounts, or how many other accounts there may be.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

An agent found a handwritten note in Ukrainian at the house. A Ukrainian-speaking agent roughly translated the heading of the note as: "How I'm Going To Manage My Ten Million Dollars." Some of the money was supposed to go to Kvashuk's father.

II. ANALYSIS

Volodymyr Kvashuk is a flight risk. Kvashuk is a twenty-five year old man charged with stealing ten million dollars. If convicted after trial, his Guidelines range could be 87-108 months or higher. The evidence is strong. Kvashuk effectively admitted felony mail fraud to Microsoft investigators, albeit at a low level. Various evidence connects him to the large-scale CSV theft, including the millions in unreported income that flowed into his accounts as the CSV was being stolen and resold. Kvashuk's claim that the money came from his father is disproven by the note found in his house showing that he planned to give some of the "Ten Million Dollars" to his father.

If released, Kvashuk will have tremendous incentive to flee to his homeland, the Ukraine. Kvashuk grew up in the Ukraine, speaks the language, and has family there. His ties to the United States, on the other hand, are limited. He has only been in this country since 2015. He has overstayed his visa. He may lose his job. Kvashuk claims to have applied for asylum, but success is far from guaranteed – especially given the pending criminal charges.

If Kvashuk goes to the Ukraine, he will be beyond the reach of U.S. law enforcement. Pursuant to the Constitution of the Ukraine, citizens of the Ukraine cannot be extradited to other nations from within its boundaries. CONSTITUTION OF UKRAINE June 28, 1996, art. 25.

Kvashuk may also have the means to flee. Of the $10 million in CSV that Kvashuk stole, over $7 million is unaccounted for. Kvashuk has used a bitcoin mixer to hide the money trail. Although the review of evidence seized from his house has just begun, agents have already found notes that suggest the existence of previously-unknown

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

accounts and bitcoin wallets, along with thousands in cash. Kvashuk's financial disclosures to Pretrial Services are essentially worthless, as he would not even discuss the source of the money he used to pay for the $160,000 car or the $1.6 million house.

In summary:

- Kvashuk has great incentive to flee;
- Kvashuk has a homeland to flee to, where he is untouchable; and
- Kvashuk's assets are unknown.

Pretrial Services is recommending release with conditions. As this Court knows, in recommending release or detention, Pretrial Services is bound by a highly restrictive set of policies. Those policies drove the recommendation in this case. As just one example, Pretrial Services cannot consider the possibility that Kvashuk has failed to disclose all of his assets. Pretrial Services must also operate on the assumption that the traditional steps to mitigate risk – such as the surrender of Kvashuk's passport – will be effective, even though experience shows that defendants can flee despite such conditions.

This Court is not bound by the policies that constrain Pretrial Services. This Court can consider the totality of the evidence, and evaluate whether conditions such as electronic monitoring and passport surrender would *actually* prevent flight. The truth is that, if Kvashuk decides to flee, there are no conditions that will stop him.

As courts have repeatedly recognized, electronic monitoring has many uses, but it does not prevent flight. *United States v. Townsend*, 897 F.2d 989, 994-95 (9th Cir. 1990) ("Nor does the wearing of an electronic device offer assurance against flight occurring before measures can be taken to prevent a detected departure from the jurisdiction."); *see also United States v. Menaged*, 2017 WL 2556828, at *4 (D. Ariz. June 13, 2017) ("If Defendant intended to flee, the GPS device could easily be removed. The device would not prevent Defendant from traveling to another country. A GPS device would not prevent him from fleeing, and thus does not ameliorate his risk of flight."); *United States v. Patel*, 2017 WL 1098822, at *2 (E.D. Wash. Mar. 23, 2017) ("The Court further finds

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

electronic home monitoring and GPS monitoring to be ineffective tools regarding the concern of flight, particularly foreign flight. When a monitoring device is removed or cut (which is what occurs when individuals flee), the Probation Officer receives an alert. However, there is no ability for the Probation Office to locate an individual and prevent them from departing the District or the country. These devices are more effective in addressing concerns related to safety of the community or other non-compliance.").

Seizing Kvashuk's passport is also no guarantee against flight. Determined fugitives regularly obtain documents or cross borders with no documentation. Kvashuk may even be able to get a new Ukrainian passport, by simply reporting that his current one was lost or stolen.

IV. CONCLUSION

For the reasons set forth above, this Court should detain Kvashuk.

DATED this 19th day of July, 2019.

Respectfully submitted,

BRIAN T. MORAN
United States Attorney

/s/ Michael Dion
MICHAEL DION
Assistant United States Attorney
700 Stewart Street, Suite 5220
Seattle, WA 98101-1271
Phone: 206-553-7729
E-mail: Michael.Dion@usdoj.gov

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

CERTIFICATE OF SERVICE

I hereby certify that on July 19, 2019, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system which will send notification of such filing to the attorney(s) of record for the defendant.

/s/ Elizabeth Gan

ELIZABETH GAN
Legal Assistant
United States Attorney's Office
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
Phone: (206) 553-4370
FAX: (206) 553-4440
E-mail: Elizabeth.Gan@usdoj.gov